

Remarks/Arguments:

Please change the attorney docket number for this matter from "NAK1-BM08" to "62478-1800".

The Office Action asserted that the original title was not descriptive. As such, this response amends the title to read "ENCRYPTION METHOD FOR ENCRYPTING PLAINTEXT DATA COMPOSED OF A PLURALITY OF BLOCKS, AND DECRYPTION METHOD FOR DECRYPTING CIPHERTEXT DATA COMPOSED OF A PLURALITY OF BLOCKS"

Claims 1-10 remain in this application.

Claims 1-10 were rejected as being anticipated by *Matsuzaki et al.* (US5351299, hereinafter "*Matsuzaki*"), or as being unpatentable over *Matsuzaki* in view of *Schneier* ("Applied Cryptography"). Applicant respectfully disagrees as the cited references do not teach, suggest, or motivate all the recitations of any of the rejected claims.

This application claims an encryption method for use by an encryption apparatus that encrypts plaintext data composed of a plurality of blocks. It does so one block at a time, and in a manner that, (a) varies between blocks, and (b) **depends on how many blocks of the plaintext data have already been encrypted**. The manner in which the handling of the blocks differs between blocks depends in part on the number of subkeys generated and used to encrypt each block. For some blocks, a group of n subkeys is generated and used, while for others a group of less than n subkeys is generated and used.

In contrast, *Matsuzaki* describes a method for encrypting a block of input data by: (a) dividing it into N sub-blocks, each sub-block having M bits; (b) manipulating the sub-blocks to form an encrypted form of the input data block; and (c) repeatedly applying steps (a) and (b) to the encrypted block resulting from any prior iterations to obtain a more strongly encrypted form of the input data block. More particularly, *Matsuzaki* describes a data encryption apparatus wherein a block of input data is divided into N sub-blocks, 1 to $N-1$ sub-blocks of which is selected by a first selection unit with a sub-block selection key. Then the selected sub-blocks of data are compressed into a single sub-block of data in a first combination unit, and encrypted with a data encryption key in an F-function unit. A second combination unit combines the sub-blocks of

data not selected in the first selection unit with the output of the F-function unit by XOR. An output unit outputs N sub-blocks of data arranged in the same order as the initial N sub-blocks, in which the 1 to N-1 sub-blocks selected in the first selection unit are outputted without any change, and the other sub-blocks being the outputs of the second combination unit. The N sub-blocks output by the output unit are the encrypted form of the input data block. The process used to form the encrypted form of the input data block can be repeated to further encrypt the input data block.

In reviewing *Matsuzaki*, it is important to realize that it does not use the term block in the same manner as the claims of this application. As such, Applicant has described *Matsuzaki* using both the term block and the term sub-block to avoid confusion. This is consistent with the language of claim 1 of this application, and with the text of *Matsuzaki*.

Claim 1 recites in part: "an encryption apparatus that encrypts plaintext data composed of a plurality of blocks, the encryption method comprising: a block obtaining step for obtaining the plaintext data one block at a time in order from outside the encryption apparatus...." Of particular note is that the data is taken (a) one block at a time, and (b) the blocks are taken in order. Figure 6 of *Matsuzaki* relates to a second embodiment described in the text beginning at column 10, line 47 which states: "The configuration of the data encryption apparatus of this embodiment is shown in FIG. 6, where 64-bit input data A is divided into four blocks: A0, A1, A2, and A3...." If one interprets the 64 bit input data as a "block", then A0, A1, A2, and A3, being segments of that block, are "sub-blocks". If the 64 bit input data is considered to be the "block" of claim 1, then *Matsuzaki* can be said to satisfy at least part of the initial portion of claim 1 that requires that blocks from outside the apparatus be obtained one block at a time.

However, with such an interpretation, *Matsuzaki* does not satisfy at least the portion of claim 1 that recites selecting a mode according to how many blocks have been obtained. Although *Matsuzaki* describes repeated operations on a block, it doesn't teach, suggest, or motivate varying those operation depending on how many blocks have preceded that block.

The Office Action asserts a different interpretation, that the initial portion of claim 1 is satisfied by element 303 of Figure 6 of *Matsuzaki*, which obtains a 32 bit block of input. However, this

assertion is incorrect as can be seen by a careful review of the recitations of claim 1 and the text and figures of *Matsuzaki*.

Matsuzaki, in describing the operation of the apparatus of figure 6, beginning at line 53 of column 10, states: "The selection unit 303 consists of a second selection unit to select any one or two blocks of data among the other three blocks of data: A0, A1, and A3 and a third selection unit to select all the other blocks." Also, beginning at line 22 of column 11, it states: "Accordingly the selection unit 303 outputs A1 as R1, and A1 and A3 as L1." As such, element 303 is simultaneously obtaining either three 16 bit blocks, or one 32 bit block and one 16 bit block. As such, if less than the 64 bits of input data is interpreted as comprising multiple blocks, *Matsuzaki* does not satisfy claim 1 as it does not obtain those blocks "one block at a time". Moreover, *Matsuzaki* does not appear to be obtaining data one block at a time in order as recited by claim 1.

Even if the Office Action was correct in asserting that element 303 satisfies the portion of claim 1 relating to obtaining plaintext data one block at a time in order from outside the encryption apparatus, *Matsuzaki* still would not satisfy all the recitations of claim 1.

Claim 1 also recites: "a selecting step for selecting either a first mode or a second mode for a current block obtained in the block obtaining step according to how many blocks have been obtained...." [emphasis added] *Matsuzaki* fails to teach, suggest, or motivate determining which of two modes of operation will be applied to a block depending on how many blocks have preceded that block. The Office Action asserts that *Matsuzaki* discloses element 302 as determining which of two blocks will be subjected to the first encryption mode with the first key. However, selection by element 302 is done according to a block selection key BK1 and some or all of the bits of A2 (see column 11, lines 15-16). As such, selection is not done according to how many blocks have been obtained.

Claim 1 also recites: "a key generating step for generating (1) a first group composed of a predetermined number n of different subkeys when the first mode is selected, and (2) a second group composed of less than n different subkeys when the second mode is selected...." [emphasis added] The Office Action asserts that this portion of claim 1 is satisfied by element

SK1 of figure 6 of *Matsuzaki*. However, simply using a subkey (or even two subkeys) does not satisfy the recitations of claim 1 which recites generating a first group and a second group of subkeys, with the groups each containing a different number of subkeys.

Claim 1 also recites: "an encrypting step for encrypting the current block by subjecting the current block to *n* conversion processes in order..." *Matsuzaki* does discuss subjecting the 64 bits of input data to multiple conversion processes, but the Office Action does not assert the 64 bits of input data is the block of claim 1. Instead, it asserts that the 32 bit combination of A1 and A3 is equivalent to the claimed block. However, *Matsuzaki* does not teach, suggest, or motivate subjecting the 32 bit block of A1 and A3 to multiple conversion processes in order. Instead, it describes converting A1 and A3 separately to form A1+D1 and A3+D1 (see figure 6), combining them with A0 and A2 to form 64 bits of data, and then selecting 16 bit portions of that data for subsequent conversion. Even if the Office Action asserted that the 64 bits of input data were the block claimed, *Matsuzaki* would not satisfy the recitations of claim 1 for at least the reasons already provided.

Claims 2-5 are patentable over the cited references at least because of their dependent on claim 1. The are also patentable at least for the reasons provided below.

Claim 2 recites in part: "the selecting step selects (i) the first mode for blocks whenever a number of blocks that have been obtained is equal to a multiple of a predetermined value, and (ii) the second mode for all other cases." The Office Action asserts that claim 2 is satisfied by *Matsuzaki* depicting the alternating use of SK1 and SK2, and asserts that SK1 is used when the number of blocks is odd, and SK2 when the number of blocks is even. However, this is an incorrect characterization of *Matsuzaki*, and is inconsistent with the arguments put forward in the Office Action in regard to claim 1. It is important to note that it is the number of blocks which determines which mode is used. Although *Matsuzaki* shows the use of SK1 and SK2 during different conversion steps, it does not teach, suggest, or motivate selecting a mode based on the number of blocks that have obtained by the apparatus. Moreover, even if selection of SK1 and SK2 was done according to the number of blocks that had been obtained, selection of SK1 and SK2 does not satisfy the mode selection recitations of claim 1 which require generation of two groups having different numbers of sub-keys.

Claim 3 recites in part: "the encryption apparatus includes an initial value storing means for storing an initial value, the encrypting step encrypts the current block to generate a ciphertext block having a predetermined length, and the key generating step generates the first group using the initial value in the first mode and generates the second group using the initial value and the ciphertext block most recently generated by the encrypting step in the second mode."

[emphasis added] The Office Action asserts SK1 and SK2 are the initial value claimed, and it is true that they are likely stored, and are used in encryption. However, the claim does not recite use of the initial value to encrypt, but to generate the first and second groups of subkeys. As the Office Action asserts that SK1 and SK2 are the first and second groups of subkeys, they cannot satisfy the recitations of claim 3 because they are not used to generate themselves. Even if some other value was asserted to be the initial value as claimed, *Matsuzaki* would not satisfy the recitations of claim 3 because it does not teach, suggest, or motivate the use of two groups of subkeys each having a different number of subkeys.

The Office Action relies on the similarities between claims 1 and 4 for rejecting claim 4, and does not provide any basis specific to claims 4 for rejecting claim 4. As such, Applicant anticipates that claim 4 will be allowed if claims 1 is allowed, and claim 1 has been shown to be patentable over the cited references.

The Office Action relies on the arguments presented in support of the rejection of claim 1 to support the rejection of claim 5. As claim 1 has been shown to be patentable over the cited references, it is anticipated that claim 5 will be allowed as well.

The Office Action relies on the similarities between claims 1-4 and 6-9 for rejecting claims 6-9, claims 6-9, and does not provide any basis specific to claims 6-9 for rejecting claims 6-9. As such, Applicant anticipates that claims 6-9 will be allowed if claims 1-4 are allowed, and claims 1-4 have been shown to be patentable over the cited references.

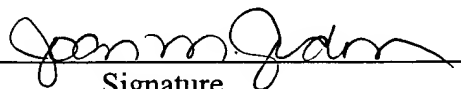
It is believed that the case is now in condition for allowance, and an early notification of the same is requested. If the Examiner believes that a telephone interview will help further the prosecution of this case, he is respectfully requested to contact the undersigned attorney at the listed telephone number.

Appl. No. 09/638,616
Amdt. dated October 8, 2004
Reply to Office action of July 12, 2004

Docket No. 62478-1800 (prev. NAK1-BM08)

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on October 8, 2004.

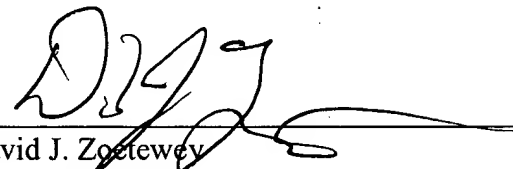
By: Joan M. Gordon


Signature

Dated: October 8, 2004

Very truly yours,

SNELL & WILMER L.L.P.


David J. Zoetewey
Registration No. 45,258
1920 Main Street, Suite 1200
Irvine, California 92614-7230
Telephone: (949) 253-4904